Case No. D073943

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
FOURTH APPELLATE DISTRICT, DIVISION ONE

The People of the State of California,

Plaintiff and Petitioner,

v.

The Superior Court of the State of California, San Diego County,

Respondent.

Florencio Jose Dominguez,

Real Party in Interest and Defendant.

On Appeal from San Diego County Superior Court,
Case No. SCD230596
The Honorable Charles Rogers, Judge

Brief of *Amici Curiae* American Civil Liberties Union and American Civil Liberties Union of San Diego and Imperial Counties In Support of Real Party in Interest Seeking Dismissal

---

Bardis Vakili (SBN 247783)
American Civil Liberties Union Foundation of San Diego and Imperial Counties
2760 Fifth Ave #300
San Diego, CA 92103
T: 619.232.2121
bvakili@aclusandiego.org

Vera Eidelman (SBN 308535)
Andrea Woods
Brett Max Kaufman
Brandon Buskey
Rachel Goodman
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
T: 212.549.2500
veidelman@aclu.org

Attorneys for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

caused—STRmix to produce wildly different results from programs purporting to calculate the same match statistic for the same suspect and crime scene sample. Moreover, access to source code has exposed serious flaws in other previously accepted probabilistic genotyping programs, as well as other algorithms used as evidence in criminal trials.

Given this, and the centrality of the STRmix test results to the State's case against Mr. Dominguez, the Fourteenth Amendment requires that Mr.

source code that plays a critical role in establishing a defendant's culpability at trial. The trial court's vindication of Mr. Dominguez's rights, which would allow the source code to become part of the record, is the first necessary step in allowing the public to exercise its constitutionally guaranteed oversight function in this case.

For these reasons and those given below, this Court should dismiss this petition and reinstate the trial court proceedings, including the discovery order.

2. BACKGROUND

STRmix, the technology at issue here, purports to do what traditional DNA testing cannot accomplish. Indeed, in this case, the prosecution tasked STRmix with identifying the perpetrator of a crime after traditional methods repeatedly failed to generate data that was conclusive or convincing to a jury.

Specifically, STRmix claims to be able to identify the perpetrator of a crime from a tiny, degraded DNA sample swimming in a mixture of multiple individuals' DNA. The problem STRmix seeks to solve is difficult. While traditional DNA analysis typically focuses on high-saturation, single-source samples—often, blood or semen collected from a crime scene—STRmix seeks to analyze samples that come from multiple contributors and are often degraded. These samples are typically "touch" samples scraped from an object multiple people have touched—for example, a purse strap, a knife handle, or, as in this case, two gloves. The precise number of contributors to such samples, as well as which specific material belongs to which contributor, is almost always unknown. And because the genetic material is often degraded or low-copy, whether data in a profile accurately reflects a genetic marker or is simply random noise may be

unclear.

This means that, while traditional DNA analysis only looks for a match to a single person's known DNA profile, STRmix must first sketch a series of profiles from the complex DNA mixture based on assumptions about the sample, including factors like how many individuals contributed to the mixture, how much of each person's DNA is present, and how old or degraded the DNA is, before looking for a match. *See* Andrea Roth, *Machine Testimony*, 126 Yale L.J. 1972, 2018–19 (2017). Essentially, traditional DNA analysis is like looking at a photograph, while STRmix's analysis is like starting with an investigator's composite sketch.

To accomplish this feat, STRmix implements an "algorithm" operationalized through "source code" to produce a "likelihood ratio." Each of these quoted terms requires elaboration.

At the most elementary level, an algorithm is a series of steps that transforms inputs into an output. *See* Thomas Cormen et al., *Introduction to Algorithms* 1 (1st ed. 1994). In essence, it is like a formula, a manual, or a recipe: a set of instructions for how to get to an end result from raw materials. "Source code" refers to the human-written instructions that tell a computer how to execute those steps.

In STRmix's case, the output or end result is a single number called a "likelihood ratio," which is computed by dividing (1) the likelihood of the crime scene evidence if the accused individual is included as a contributor, by (2) the likelihood of the evidence if a random person is included instead. *See* William C. Thompson et al., *Forensic DNA Statistics: Still Controversial in Some Cases*, Legal Studies Research Paper Series No. 2013-122, 23 n.17 (Dec. 2012), *available at* https://perma.cc/J6Q6-45R2. In other words, the ratio reflects the likelihood of the evidence if the

prosecution's theory (i.e., the accused individual contributed to the DNA) is correct divided by the likelihood of the evidence if the prosecution's theory is wrong (i.e., he did not).

Unlike its output, STRmix's inputs are not fully known—and this is one of the problems at the crux of this case. Based on the record, the program decides whether something identified in a DNA sample constitutes stutter (i.e., random noise that can be ignored) or an actual allele (i.e., a characteristic that the suspect must match). Pet. Exhibit H at 98. It also appears to offer the ability to test the hypothesis that contributors are related. RPI Exhibit 5 at 429. And STRmix appears to allow analysts to choose the number of contributors to a particular sample. Pet. Exhibit H at 97. Inputs may also include assumptions about the quantity of DNA from each contributor, and the race or ethnicity or other statistical properties of the comparison population.

STRmix is used by the largest number of U.S. crime labs, but it is not the only algorithm that seeks to generate likelihood ratios from complex DNA mixtures. *See* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 Stan. L. Rev. 1343, 1422 (2018). Other for-profit ventures include TrueAllele, which had been used in approximately 500 criminal cases by late 2016. *See* Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy Over the Reliability of Automated Forensic Techniques*, 66 DePaul L. Rev. 97, 100–01 (2016). And government actors have also developed such programs, like New York's Forensic Statistical Tool ("FST").

These organizations, including government actors, have asserted a private property interest in their work. *See* Lauren Kirchner, *Traces of*

beings—including the one on trial in this case—behind bars or even render them eligible for death. But such algorithms, too, differ in their underlying assumptions, inputs, and training datasets—all things the State seeks to keep secret here. And if the underlying pieces differ, so too must the quality of their output.

To an extent, validation studies may reveal these differences. Such studies are meant to test the validity of a program under certain, defined conditions. Internal validation studies, like the ones the State refuses to disclose in this case, may reveal errors and bugs. And external validation studies, like the ones the State has not fully provided to the defense in this case, may offer additional insight because they are conducted by individuals with fresh eyes, who were not involved in building the program. But validation studies alone are not enough for effective defense review because validation studies are constrained by the specific conditions they test. For example, a radar gun that has been validated only against individual automobiles on a test driving range cannot be deemed valid for measuring the speed of a skateboarder on a busy street; it could be accurate, but the only way to know is to specifically test the machine for that use.

To fully confront and put evidence derived from STRmix to the adversarial test, access to its validation studies; underlying model; training data; source code; input parameters and data specific to each case; and any other results from which the final, reported result was chosen is necessary. As explained in further detail below, the algorithm's underlying model reflects the theory and intended process behind the probabilistic analysis, while the source code shows how that intended process has been put into practice. For example, the source code could reveal that concepts not included in the underlying model have somehow been included in the

program; that optimizations meant to, for example, minimize use of the computer’s memory inadvertently change output; and that the code includes accidental mistakes. The training data constitutes the dataset on which the algorithm practiced to learn the probabilities it uses; the input parameters and data specific to each case shows the assumptions, human decisions, and raw inputs used to generate a particular likelihood ratio; and any other results calculated offer comparisons for the ultimate result communicated nd rs

during testing—that directly affect interpretation." Roth at 1996–97.

On the machine learning side, humans also impact the algorithm's design by, for example, choosing the training data—a decision that can significantly affect the algorithm's output in ways that differ for suspects of different races, ethnicities, or ancestral backgrounds. *See, e.g.*, *People v. Collins*, 15 N.Y.S.3d 564, 580–81 (N.Y. Sup. Ct. 2015) (crediting objection of two defense experts to FST because (1) it was trained on data with only "Asian, European, African, and Latino" categories, which is inadequate for identifying other races or ethnicities, and (2) the training data appeared to include only three Asian individuals, which was insufficient to determine false positive rates for people with Asian ancestry); Roth at 1997 (discussing the importance and difficulty of identifying "the appropriate reference population for generating estimates of the rarity of genetic markers"); *see also* Lauren Kirchner, *ProPublica Seeks Source Code for New York City's Disputed DNA Software*, ProPublica (Sept. 25, 2010of

Should It Take for Us to Trust It?, *in* Trust and Trustworthy Computing 396, 397 (Alessandro Acquisti et al., eds., 2010)). The risk of bugs only

themselves have recognized that "you will get a different likelihood ratio every time you . . . put the same data in." *People v. Bullard-Daniel*, 42 N.Y.S.3d 714, 725 (N.Y. Cty. Ct. 2016).

At each of these stages, people—as they do—will almost certainly make mistakes. For example, with regard to the coding stage, one study found that even highly experienced programmers make a mistake in "almost 1% of all expressions contained in [their] source code." Chessman at 186–87. Mistakes occur even with tasks as simple as inputting "yes" or "no" to match a program's parameters to a particular case.

complex as probabilistic DNA typing embodied in source code, people may simply have conceptual blind spots. The fact that STRmix combines several complex areas of expertise—genetics, forensic science, statistics, and programming—suggests that ESR employees, while expert in one, may make errors due to an incomplete grasp of the other. Chessman at 188.

Moreover, financial incentives may pervert the goals of companies that build probabilistic genotyping algorithms. These dynamics are particularly acute in the field of probabilistic genotyping, where the prosecution, backed by the superior resources of the state, is by far the most frequent and reliable customer. That customer is likely to be most satisfied with an algorithm that delivers a match, and is less likely to question its results. Therefore, private companies may be incentivized to find a match, rather than the truth, in order to attract and retain these customers. *See Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 318 (2009) ("A forensic analyst responding to a request from a law enforcement official may feel pressure—or have an incentive—to alter the evidence in a manner favorable to the prosecution."). Market forces will predictably bias results in this direction, notwithstanding the companies' best intentions. Compounding that problem, private companies are also motivated to push for secrecy—as evidenced by this case—which keeps all of these errors hidden from the public. *See also* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. Rev. Online 101, 106 (2017), http://www.nyulawreview.org/sites/default/files/Joh-FINAL_0.pdf.

Not surprisingly, given these multiple potential sources for error, criminal justice algorithms often fail to meet the needs of a rigorous and fair judicial system. In just the last few years, researchers documented a

coding error in STRmix that had enormous consequences: it produced incorrect results in 60 criminal cases in Australia, altering likelihood ratios by a factor of 10 and forcing prosecutors to replace 24 expert statements in criminal cases. David Murray, *Queensland Authorities Confirm 'Miscode' Affects DNA Evidence in Criminal Cases*, Courier-Mail, Mar. 20, 2015, http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b. STRmix has documented at least seven additional bugs that affect its reported likelihood ratio, occasionally by more than an order of magnitude. RPI Exhibit 6 at 430–31. In addition, ESR has issued numerous new versions of STRmix—including at least one new version since the SPDP crime lab calculated some of its results in this case—to fix identified bugs.

Access to the source code of other probabilistic genotyping algorithms—precisely what the defendant seeks here—has revealed additional errors. In New York, after a federal court ordered the release of FST's source code to the defense, an expert witness discovered that "the program dropped valuable data from its calculations, in ways that users wouldn't necessarily be aware of, but that could unpredictably affect the likeliho-4.25cnt.DRdditional 6ars neT its cj (6a22t DN)-A be 8 wi9 0 9.3(5.269 .7(rs)DtSo)-

jeopardy by faulty coding, and for prosecutors, whose cases can be upended by their introduction of unreliable evidence.

Indeed, notwithstanding the fact that each probabilistic DNA algorithm claims to provide accurate results based on objective scientific principles, competing programs frequently reach different results for the same underlying data. For example, in one case, STRmix and TrueAllele generated vastly different results for the same crime scene sample and suspect: TrueAllele found no statistical support for a match, while STRmix generated a likelihood ratio of 300,000. *See* Roth at 2019–20. As a result, the court excluded the STRmix results from trial. See *New York v. Hillary*, No. 2015-15 (N.Y. Cty. Court Aug. 26, 2016).[3] In another case, as discussed above, FST calculated a likelihood ratio of 172 million, while STRmix calculated a likelihood ratio of 10 trillion. *Seepersad*, 2018 WL 1163820, at *1.

Plainly, algorithms are fallible. While this may surprise laypeople, computer scientists, the creators of algorithms, have long been acutely aware of it. They caution that "the evidence produced by computer programs is no more inherently reliable or truthful than the evidence produced by human witnesses." Chessman at 185.

Yet when these algorithms are introduced in the courtroom, legal experts and prosecutors suggest that they are infallible and that their results are foolproof, "overstat[ing] the probative value of their evidence, going far beyond what the relevant science can justify." President's Council of

---

[3] *Available at* www.northcountrypublicradio.org/assets/files/08-26-16DecisionandOrder-DNAAnalysisAdmissibility.pdf.

public, must be given the opportunity to explore that degree of accuracy if our criminal system is to reach just results.

3(B) <u>Denying an accused individual access to an algorithm that will be used to generate material evidence against him in a criminal trial violates his Fourteenth Amendment right to due process.</u>

The Fourteenth Amendment right to due process guarantees, "in essence, the right to a fair opportunity to defend against the State's accusations." *Chambers v. Mississippi*, 410 U.S. 284, 294 (1973). Due process "speak[s] to the balance of forces between the accused and his accuser" and requires that discovery be a "two-way street." *Wardius v. Oregon*, 412 U.S. 470, 474, 475 (1973). When the State's accusations are premised on the results of computerized algorithms, rather than simpler pieces of evidence, maintaining that due process balance and affording the defense a "fair opportunity to defend against the State's accusations" must include pre-trial access to information about the algorithm.

As state supreme courts have recognized with regard to traditional DNA testing, "fair trial and due process rights are implicated when data relied upon by a laboratory in performing [DNA] tests are not available to the opposing party for review and cross examination" pretrial. *State v. Schwartz*, 447 N.W.2d 422, 427 (Minn. 1989); *Ex parte Perry*, 586 So. 2d 242, 255 (Ala. 1991) (requiring disclosure of full details of DNA analysis methodology and holding "defendant's fair trial and due process rights . . . clearly require that the prosecution allow the defendant access to the DNA evidence"). Given the potential complexity of the DNA tests at issue here, the same must hold true for probabilistic genotyping algorithms.

Due process is concerned with all evidence "material either to guilt or to punishment." *Brady v. Maryland*, 373 U.S. 83, 87 (1963). "It is well settled that the government has the obligation to turn over evidence in its

defendant." Order as to Kevin Johnson at 1, *United States v. Johnson*, No. 1:15-cr-00565-VEC (S.D.N.Y. June 7, 2016), ECF No. 57; *see also* Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing, *United States v. Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. May 18, 2016), ECF No. 205 (holding that source code underlying technique used to identify defendant was material and defendant therefore has a right to access it before the trial); *see also* Order Denying Dismissal and Excluding Evidence, *Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. May 25, 2016), ECF No. 212.[4]

The defendant's rights to access this information cannot be satisfied by the constrained access the State and ESR have offered in this case. ESR

---

[4] The State argues that accepting Mr. Dominguez's position in this case would mean that Microsoft Excel's source code would be discoverable in any financial crimes case in which the government uses the Excel program to conduct forensic accounting to make its case. Pet.'s Br. at 10. This analogy misses the mark. In a financial crimes prosecution involving a spreadsheet, the relevant algorithms would likely be the specific formulas used to calculate relevant evidence (e.g., "Cell A4 contains the expression '=SUM:A1-A23'"), not the source code to Excel. Such formulas are commonly understood, and can be extracted from the spreadsheet and verified without access to Excel software (e.g., they can be calculated by hand, or with another spreadsheet tool such as LibreOffice Calc.). Just as a spreadsheet is operationalized by a program like Excel or Calc, a Java program like STRmix is operationalized by the Java Virtual Machine (JVM). The defense is asking for the STRmix source, not for the JVM source. Returning to the spreadsheet analogy: in a case where the spreadsheet's calculation is relevant to the State's case in chief, arguing that its formulas are protected by the trade secrets privilege would be folly. And yet that is what the State and ESR are effectively arguing here, in addition to the argument that any technical explanation of how to use Excel also cannot be disclosed because it is copyrighted.

makes “STRmix . . . available for purchase” by the defense, and also offers defense experts access to the source code of the particular version of STRmix used in the defendant’s case—but only after the defense expert signs a confidentiality agreement and agrees to conduct any review under direct supervision by the company in an agreed-upon room and through handwritten notes alone. Pet. Exhibit I at 181–82. The court in *Johnson* refused to approve nearly identical constraints, which it described as “strict” and

In the civil context, courts have held that government reliance on secret, proprietary algorithms violates due process. *See K.W. v. Armstrong*, 180 F.

33 (Cal. 1997) (trial court maintains broad discretion to continue trial in light of introduction of evidence not disclosed until trial). This is particularly true where, as here, the state's evidence may be complicated and relatively novel, requiring more time to prepare an adequate cross examination.

3(C) <u>If the secret algorithm is not disclosed at this stage, the defendant's Sixth and Fourteenth Amendment rights to confrontation and a fair trial will be implicated at trial.</u>

If this Court were to overturn the trial court's grant of access to STRmix's source code, Mr. Dominguez's Sixth Amendment right to confront "the witnesses against him," U.S. Const. amend. VI, and his Fourteenth and Sixth Amendment rights to a fundamentally fair process would be implicated at trial. While those rights are not at direct issue in this appeal, they will almost certainly come up at trial should the State's writ be granted.

"Whether rooted directly in the Due Process Clause of the Fourteenth Amendment or in the Compulsory Process or Confrontation Clauses of the Sixth Amendment, the Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense." *Holmes v. South Carolina*, 547 U.S. 319, 319 (2006) (quoting *Crane v. Kentucky*, 476 U.S. 683, 690 (1986)) (quotation marks omitted). Broadly speaking, "a fair trial is one in which evidence subject to adversarial testing is presented to an impartial tribunal for resolution of issues defined in advance of the proceeding." *Strickland v. Washington*, 466 U.S. 668, 685 (1984).

In addition to the due process concerns discussed in section 3(B) *supra*, several other strands of the due process doctrine will become relevant at trial. First, with respect to evidence withheld from a defendant, due process

as a trial resulting in a verdict worthy of confidence," *Kyles v. Whitley*, 514 U.S. 419, 434 (1995). In addition, due process requires rejection of asymmetrical evidentiary rules—that is, those that place the prosecution's evidence in a more favorable position than the defendant's. *See Holmes*, 547 U.S. at 331. Finally, due process protects the right to cross-examine witnesses—including adversarial testing of the source code upon which they rely—in part because the jury must be empowered to "judge for itself whether [ ] testimony [is] worthy of belief." *Chambers*, 410 U.S. at 295.

Relatedly, the Confrontation Clause's animating concern is "to ensure the reliability of the evidence . . . by subjecting it to rigorous testing." *Maryland v. Craig*, 497 U.S. 836, 845 (1990). The Supreme Court has recognized that this concern applies with full force to forensic evidence. *Melendez-Diaz*, 557 U.S. at 313 (holding that affidavits reporting the results of a forensic analysis of seized drugs are testimonial and subject to the Confrontation Clause); *Bullcoming v. New Mexico*, 564 U.S. 647, 663–64, 666 (2011) (holding that certification on a forensic laboratory report is testimonial and defendant has a right to confront the specific analyst who made the certification).

The Sixth Amendment also guarantees a defendant the right "to have compulsory process for obtaining witnesses in his favor." U.S. Const. amend. VI. At a minimum, compulsory process means that criminal defendants have "the right to put before a jury evidence that might influence the determination of guilt." *Ritchie*, 480 U.S. at 56.

If this Court grants the State's writ, Mr. Dominguez's confrontation right will almost certainly be violated at trial because his lack of access to STRmix's source code will unduly inhibit his ability to confront any witness testifying about the program's results. Effectively confronting such

testimony necessarily requires that the defense access and confront STRmix's source code.

To be sure, the California Supreme Court held in *People v. Lopez* that mechanical printouts of raw data are not statements, and that "a machine cannot be cross-examined." *People v. Lopez*, 286 P.3d 469, 478 (Cal. 2012). That case held that the results of a blood alcohol analysis performed by a gas chromatography machine were not testimonial under *Crawford v. Washington*, 541 U.S. 36 (2004). *Lopez*, 286 P.3d at 478–79. It did not address the question that will be presented if this writ is granted—whether a court violates a defendant's right to confront an expert by denying him

calculate the likelihood ratio; similarly, the crime lab did not generate the methodology by which the calculation was done, nor did it build the program that generated the statistics. *See United States v. Washington*

coding errors—both deliberate and benign—are an inherent and significant part of programming. Roth at 1994; *see generally* Chessman at 183–99 (discussing various forms and frequencies of programming errors). As discussed above, consequential coding errors have been discovered in probabilistic genotyping programs once they were subject to outside scrutiny. *See* §§ 3(A) and (B), *supra*. These are the very sorts of evils confrontation is meant to deter. *Melendez-Diaz*, 557 U.S. at 318–19.

The assertion of an evidentiary privilege does not end these constitutional inquiries. *Ritchie*, 480 U.S. at 57. Indeed, the Supreme Court has held that, to preserve the "fundamental fairness of trials," material information covered by an evidentiary privilege should nonetheless have been provided to a criminal defendant, even where it consisted of extremely sensitive information in a state agency's child abuse investigation file. *Id*. at 56–57; *see also Chambers*, 410 U.S. at 302 (cautioning that "[m]echanistic[]" application of hearsay rule to exclude evidence "critical" to a criminal defendant's case can "defeat the ends of justice" and violate due process); *Green v. Georgia*, 442 U.S. 95, 97 (1979).

Nor is it any answer, as the State offers, that the source code and internal validation studies are unnecessary because STRmix's general methodology has been validated. As an initial matter, the State should not be able to rest its argument on validation studies—including STRmix's internal validation and modification studies and the SPDP crime lab's validation studies—that are not disclosed in full to the defense. In addition, as discussed above, defense access to the sort of source code at issue here has proven its worth in circumstances where validation studies were already available. *See* § 3(B), *supra* (discussing *United States v. Johnson*, No. 1:15-cr-00565-VEC (S.D.N.Y. 2016)).

believes it did, and it could be mistaken. Evaluation of the source code, in contrast, would allow the defense to verify that the validations were done correctly and reflect the same scientific expectations.

But even if SPDP's studies were superior, the existence of an alternative way to challenge STRmix's results would not change the fact that "the Constitution guarantees one way: confrontation." *Melendez-Diaz*, 557 U.S. at 318. Here, meaningful confrontation will require defense access to the source code. All complex software has errors, and ESR's admission that there have been errors in the code show that STRmix is no exception. RPI Exhibit 6 at 430–31.

At its root, this case reveals the strong parallels between black-box technologies like STRmix and the *ex parte* examinations that motivated the

Co. v. Superior Court (“*Press-Enter. II*”), 478 U.S. 1, 13, 14–15 (1986) (quoting *Press-Enter. Co. v. Superior Court* (“*Press-Enter. I*”), 464 U.S. 501, 510 (1984)); *see also Globe Newspaper*

This would achieve one of the main purposes of the First Amendment right of access, which attaches to criminal trials to allow the public to observe and evaluate the workings of the criminal justice system—and to make changes in order to eliminate injustice. See *id*. at 572. As the Supreme Court has explained, "the criminal justice system exists in a larger context of a government ultimately of the people, who wish to be informed about happenings in the criminal justice system, and, if sufficiently informed about those happenings, might wish to make changes in the system." *Gentile v. State Bar of Nev*., 501 U.S. 1030, 1070 (1991). The need for public oversight of government process is strongest in criminal trials, where the state wields its greatest power to affect individual liberty. Public access "enhances the quality and safeguards the integrity" of the judicial process, "heighten[s] public respect" for that process, and "permits the public to participate in and serve as a check upon the judicial process." *Globe Newspaper*, 457 U.S. at 606.[5]

Under the Supreme Court's prevailing "experience and logic" test, the public's First Amendment right of access attaches to judicial proceedings and records where (a) the type of judicial process or record sough7s ed,e Surds the inte eval; 12cf

As the Ninth Circuit recognized in *Woodford*, meaningful access to a proceeding means access to its nuts and bolts. In *Woodford*, a lethal injection case, that meant a right to view "executions from the moment the condemned is escorted into the execution chamber." 299 F.3d at 870–871, 877. The court explained that, for the right of access to accomplish its goals, citizens must have reliable information about the 'initial procedures,' which are invasive, possibly painful and may give rise to serious complications." *Id.* at 876–77. The same must be true for algorithms that produce the prosecution's material evidence in a criminal trial—which also have the potential for serious complications and inaccuracies. Just as without access

Moreover, the work of one legal scholar suggests that limiting access on the basis of a purported trade secret privilege would be ahistorical. Rebecca Wexler has found that "[e]arly historical sources suggest that the [trade secrets] privilege"—precisely the tool companies are now using to keep algorithms out of the record of criminal cases—was historically "unavailable in criminal proceedings." Wexler at 1388–90. Rather, historically, when courts were asked to conceal trade secrets

evidence establishing its invalidity. “Since a series of high-profile legal challenges in the 1990s increased scrutiny of forensic evidence, a range of long-standing crime-lab methods have been deflated or outright debunked,” including bite-mark analysis, ballistics testing, fingerprinting, and microscopic-hair-comparison. Shaer, *The False Promise*, *supra*.

Indeed, the Supreme Court has relied on public scrutiny of forensic processes to inform its interpretation of constitutional protections. *See Melendez-Diaz*, 557 U.S. at 319 (“Serious deficiencies have been found in the forensic evidence used in criminal trials.”). And state supreme courts—as well as federal appellate courts—have equally looked to work done by the public, rather than either party or its experts in a criminal case, to determine that evidence based on specific technologies was not sufficiently reliable to be admissible into evidence. *See, e.g.*,

Allowing the public, including academics and other experts, to examine DNA typing evidence would markedly

enjoy a presumption of openness in the criminal justice system. *See, e.g.*, *In re Application of WFMJ Broad. Co.*, 566 F. Supp. at 1040 (tapes played to jury in open court); *United States v. Posner*, 594 F. Supp. 930, 934–35 (S.D. Fla. 1984) (tax returns admitted into evidence); *United States v. Scott*, 48 M.J. 663 (A. Ct. Crim. App. 1998) (materials entered into evidence at trial); *Valley Broad. Co. v. U.S. Dist. Court*, 798 F.2d 1289, 1292–93 (9th Cir. 1986) (transcripts of exhibits); *In re Times-World Corp*., 488 S.E.2d

incorporate discovery materials into substantive litigation. Indeed, in the civil context courts have held that under the First Amendment, reports relied upon by parties in the "adjudication stages" of litigation are presumptively "available for public inspection unless exceptional circumstances require confidentiality." *In re Continental Ill. Sec. Litig.*, 732 F.2d 1302, 1314 (7th Cir. 1984); *accord Joy v. North*, 692 F.2d 880, 893 (2d Cir. 1982); *see also Rushford*, 846 F.2d at 253 (documents filed in connection with summary judgment motion); *NBC Subsidiary (KNBC-TV), Inc. v. Superior Court*, 980 P.3d 337, 360 n.28 (Cal 1999) (applying the same principle in a civil context).[9] Those principles apply with even greater force in the criminal context to evidence and its attendant documents, *see, e.g.*, *In re Wash. Post Co.*, 807 F.2d at 389–90 —and, assuming this case proceeds to trial or any proceeding or briefing that adjudicates substantive rights, this would encompass information about an algorithm that produces the evidentiary results at the center of the State's case against Mr. Dominguez. *See Doe*, 749 F.3d at 267.

As discussed above, the "logic" prong also dictates that the First Amendment right of access attaches in this context. Public access to the highly complex algorithmic source code that produced the evidence that will be used against Mr. Dominguez at trial would "enhance[] the quality and safeguard[] the integrity of the factfinding process, with benefits to both the defendant and to society as a whole," *Globe Newspaper Co.*, 457 U.S. at

606; *see also, e.g.*, *Grove Fresh Distribs., Inc. v. Everfresh Juice Co.*, 24 F.3d 893, 897 (7th Cir. 1994) (citing *Richmond Newspapers*, 448 U.S. at 555); *Int'l Fed'n of Prof'l & Tech. Eng'rs, Local 21, AFL-CIO v. Superior Court*, 42 Cal. 4th 319, 333 (2007).[10]

iii. The court may limit the public's access to information about the algorithm, but any limitations must be narrowly tailored to comport with the First Amendment.

Of course, the fact that the First Amendment right of access will *attach* to algorithmic source code properly entered into the record does not dictate that the source code itself will be made public, in part or in its entirety. Because the right is a qualified one, the outcome (in this case or any other) will depend upon the strength of the government's interest in continued hinino(in)-9.3t)

"circumstances" in which "the right to an open trial may give way . . . to other rights or interests . . . will be rare." *Waller*, 467 U.S. at 45. Such sufficiently weighty rights and interests might include, for example, "the defendant's right to a fair trial or the government's interest in inhibiting disclosure of sensitive information." *Id.* But the government's interest in this case and those like it does not approach that class of gravity. To the contrary, the defendant's right to a fair trial dovetails—rather than conflicts—with the public's right of access. *See supra* § 3(C).

Here, the government's only interest in secrecy appears to be derivative of a business's intellectual-property interest in purported trade secrets and copyrighted information. This private interest, on its own, will likely fail strict scrutiny. The Supreme Court has "recognized that the First Amendment interests served by the disclosure of purely private information like trade secrets are not as significant as the interests served by the disclosure of information concerning a matter of public importance." *DVD Copy Control Ass'n v. Bunner Inc.*, 31 Cal. 4th 864, 883 (2003) (citing *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759 (1985)). In fact, because the private "makers are under a scientific obligation to release this information for peer review," the validity of the interest is questionable. Jennifer N. Mellon, *Manufacturing Convictions: Why Defendants Are Entitled to the Data Underlying Forensic DNA Kits*, 51 Duke L.J. 1097, 1119 (2001).

. As one commentator, William Thompson, put it, "If scientific evidence is not yet ready for both scientific scrutiny and public re-evaluation by others, it is not yet ready for court." *Id.* (quoting William C. Thompson, *Evaluating the Admissibility of New Genetic Identification Tests: Lessons from the "DNA War,"* 84 J. Crim. L. & Criminology 22, 100

(1993)). As for the purported copyright interest, the introduction of copyrighted material in court will not prevent the business from enforcing its copyright anywhere else.

Moreover, "forc[ing the public] to rely on the same [government] officials who are responsible for [presenting the evidence in court] to disclose and provide information about any difficulties with the [evidence]" does not comport with the First Amendment's requirement of narrow tailoring. *Woodford*, 299 F.3d at 880.

This makes it very likely that the public's oversight role would be realized in one form or another. Regardless, the complete denial of source code used on the public's behalf to seek to convict a criminal defendant would surely be an "exaggerated response" to private-interest concerns. *Woodford*, 299 F.3d at 880. In the context of the First Amendment analysis, the compelling nature of private concerns like trade secrets will be highly suspect when balanced against the momentous and bedrock constitutional rights held by a criminal defendant and the public.

CERTIFICATE OF COMPLIANCE

I certify that the text in the attached Brief contains 12,843 words—as calculated by Microsoft Word, including footnotes but not the caption, the table of contents, the table of authorities, signature blocks, or this certification—and that this document was prepared in a 13-point Times New Roman font. *See* Rule of Court 8.204(c)(1), (3).

Dated: July 2, 2018

BY: */s/ Vera Eidelman*

Vera Eidelman (SBN 308535)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
T: 212.549.2500
veidelman@aclu.org